TNO-rapport
FEL-97-A066

Evaluatie KL informatiebeveiligings-methodieken in relatie tot het Voorschrift Informatiebeveiliging Rijksdienst (VIR)

TNO Fysisch en Elektronisch Laboratorium

Oude Waalsdorperweg 63
Postbus 96864
2509 JG 's-Gravenhage

Telefoon 070 374 00 00
Fax 070 328 09 61

Datum
april 1997

Auteur(s)
Ing. P.J.A. Verhaar

Rubricering

Vastgesteld door	:	Ing. J.P.H.M. Klomp
Vastgesteld d.d.	:	10 maart 1997
Titel	:	Ongerubriceerd
Managementuittreksel	:	Ongerubriceerd
Samenvatting	:	Ongerubriceerd
Rapporttekst	:	Ongerubriceerd

Exemplaarnr.	:	8	
Oplage	:	54	
Aantal pagina's	:	52	(excl. RDP & distributielijst)
Aantal bijlagen	:	-	

TNO Fysisch en Elektronisch Laboratorium is onderdeel van de hoofdgroep TNO Defensieonderzoek waartoe verder behoren:

TNO Prins Maurits Laboratorium
TNO Technische Menskunde

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO

Managementuittreksel

Titel	:	Evaluatie KL informatiebeveiligingsmethodieken in relatie tot het Voorschrift Informatiebeveiliging Rijksdienst (VIR)
Auteur(s)	:	Ing. P.J.A. Verhaar
Datum	:	april 1997
Opdrachtnr.	:	A94KL646
IWP-nr.	:	761.3
Rapportnr.	:	FEL-97-A066

Sinds enige tijd is het 'Voorschrift Informatiebeveiliging Rijksdienst' (VIR) van kracht voor alle overheidsorganisaties. Door de Beveiligings Autoriteit (BA) van het Ministerië van Defensie is het 'Beleidsdocument Informatiebeveiliging' opgesteld. Dit document is opgesteld naar aanleiding van het VIR en is voor de gehele Defensie organisatie van kracht verklaard. Dit houdt in dat de Koninklijke Landmacht (KL) verplicht is een informatiebeveiligingsbeleid te voeren dat minimaal voldoet aan het VIR. De werkzaamheden die binnen het VIR worden beschreven hebben tot doel het opstellen van een Informatie Beveiligings Plan (IBP) voor elk informatiesysteem en/of verantwoordelijkheidsgebied binnen een organisatie. In dit IBP worden o.a. alle te treffen en/of getroffen maatregelen beschreven of er wordt verwezen naar de plaats waar deze maatregelen zijn beschreven.
Binnen de Koninklijke Landmacht (KL) zijn methodieken ontwikkeld die eveneens tot doel hebben om te komen tot een Informatie Beveiligings Plan (IBP). Eén van deze methodieken is de 'Handleiding voor het uitvoeren van het InformatieBeveiligings Proces' (HIBP). De HIBP is ontwikkeld door de sectie Commandovoering en Informatie Voorziening van de afdeling Beleids Ontwikkeling van de LAndmachtStaf (LAS/BO/CIV) voorheen Directie Operatiën (DOKL/CIV).
Een andere methode is de 'KL-methodiek Integrale VeiligheidsZorg management' (IVZ-management). De KL-methodiek IVZ-management is ontwikkeld door de Project-Organisatie Bewakingssysteem KL 98 van het NATionaal COmmando (NATCO/PO BKL 98). Deze methodiek heeft echter een breder doel dan de HIBP, namelijk: het uitvoeren van alle management activiteiten op het gebied van bewaking en beveiliging.
LAS/BO/CIV heeft TNO-FEL verzocht de twee ontwikkelde methodieken te toetsen aan het beleidskader dat wordt geschetst in het 'Beleidsdocument Informatiebeveiliging' van de BA. Dit beleidsdocument is opgesteld naar aanleiding van het VIR. De KL-methodiek IVZ-management is getoetst voor dat deel dat betrekking heeft op informatiebeveiliging. In eerste instantie is onderzocht of de werkzaamheden die in het VIR zijn beschreven zijn terug te vinden in de KL-methodieken. Hierbij is gekeken naar overeenkomsten en verschillen in de methodieken. Naast een onderzoek naar tekortkomingen van de KL-methodieken is ook gekeken naar de efficiëntie van deze methodieken.

Daarnaast is een onderzoek uitgevoerd naar de toepasbaarheid van de in de HIBP opgenomen processen voor het bepalen van de feitelijke/vereiste beschikbaarheid, integriteit en vertrouwelijkheid.
Het onderzoek heeft tot de volgende conclusies geleid:

- het VIR is geschreven op een hoog abstractieniveau. De HIBP en de KL-methodiek IVZ management zijn praktisch ingesteld;
- voor alle methoden geldt dat de verantwoordelijkheid voor het uitvoeren van de activiteiten binnen deze methoden ligt bij het (lijn)management;
- het VIR en de HIBP beperken zich beiden tot informatiebeveiliging. De KL-methodiek IVZ-management, daarentegen, is een methodiek die de werkzaamheden beschrijft om te komen tot een adequate beveiliging, in de breedste zin van het woord, van een KL object, lokatie, eenheid of afdeling;
- het VIR en de HIBP hebben het opstellen van een Informatie Beveiligings Plan (IBP) tot doel. De KL-methodiek IVZ-management heeft tot doel dat een bundeling van plannen wordt opgesteld. Eén van die plannen binnen deze bundeling is een IBP;
- uit de KL-methodiek IVZ-management kan worden opgemaakt dat de invulling van een IBP kan (dient te) worden uitgevoerd conform de HIBP of de MP 10-10 deel 6;
- het VIR en de HIBP gebruiken verschillende benamingen voor dezelfde begrippen;
- het VIR geeft aan dat op beleidsniveau de informatiebeveiligingsaspecten geclassificeerd dienen te worden, maar geeft zelf geen classificering aan. Binnen de HIBP en de KL-methodiek IVZ-management worden de informatiebeveiligingsaspecten wel geclassificeerd;
- met behulp van de subprocessen 1 t/m 5 van de HIBP kan een afhankelijkheidsanalyse, zoals deze beschreven staat in het VIR, worden uitgevoerd. Hierbij dient opgemerkt te worden dat voor het bepalen van de maximaal toelaatbare schade en de mogelijke schade subproces 4 van de HIBP aangevuld kan worden met de waarde-incident methode en de INCI-DETAR methode van de KL-methodiek IVZ-management en de MP 10-10 deel 6;
- het identificeren en analyseren van bedreigingen kan worden bereikt door subproces 8 van de HIBP uit te voeren. De naam van dit subproces 'Uitvoeren kwetsbaarheidsanalyse' geeft verwarring met de kwetsbaarheidsanalyse volgens het VIR, waarin andere werkzaamheden worden beschreven;
- met de subprocessen 6, 7, 9 en 10 van de HIBP is het mogelijk een kwetsbaarheidsanalyse volgens het VIR uit te voeren;
- voor het opstellen van een Informatie Beveiligings Plan (IBP) kan worden voldaan door de subprocessen 11 en 12 van de HIBP uit te voeren;
- door een herindeling van de subprocessen uit te voeren zal de HIBP beter passen binnen de richtlijnen van het VIR. Bij het herindelen van de subprocessen van de HIBP zal tevens onderzocht moeten worden of een uitvoeringsvolgorde van de heringedeelde subprocessen van toepassing is;

- de processen voor het bepalen van de feitelijke/vereiste beschikbaarheid, integriteit en vertrouwelijkheid dienen vereenvoudigd te worden door het aanbrengen van wijzigingen.

Het rapport sluit af met de volgende aanbevelingen:

- om in de toekomst verwarringen te voorkomen wordt aanbevolen de begrippen in de HIBP te benoemen conform het VIR;
- pas de indeling van de huidige subprocessen van de HIBP als volgt aan:
  - wijzig de naam van subproces 8 van de HIBP (Uitvoeren kwetsbaarheidsanalyse) in bijvoorbeeld 'Uitvoeren dreigingenanalyse';
  - voeg de subprocessen 6, 7, 9 en 10 samen tot een subproces en noem dit nieuwe subproces 'uitvoeren kwetsbaarheidsanalyse;
  - pas subproces 11 aan door alleen de opsomming van maatregelen of een verwijzing naar de documenten waar deze maatregelen staan vermeld op te nemen in het IBP;
- voor vereenvoudiging van de processen voor het bepalen van de feitelijke/vereiste beschikbaarheid, integriteit en vertrouwelijkheid wordt aanbevolen deze processen te modificeren door middel van de in het rapport aangegeven wijzigingen.

Samenvatting

Door de Beveiligings Autoriteit (BA) van het Ministerië van Defensie is het 'Beleidsdocument Informatiebeveiliging' opgesteld. Dit document is opgesteld naar aanleiding van het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en is voor de gehele Defensie organisatie van kracht verklaard. LAS/BO/CIV heeft TNO-FEL verzocht twee KL-beveiligings methodieken te toetsen aan het beleidskader dat wordt geschetst in dit beleidsdocument. Het betreft de methodieken: de 'Handleiding voor het uitvoeren van het InformatieBeveiligings Proces' (HIBP) opgesteld door de sectie Commandovoering en Informatie Voorziening van de afdeling Beleids Ontwikkeling van de LAndmachtStaf (LAS/BO/CIV) voorheen Directie Operatiën (DOKL/CIV) en de 'KL-methodiek Integrale VeiligheidsZorg management' (IVZ-management) opgesteld door de Project-Organisatie Bewakingssysteem KL 98 van het NATionaal COmmando (NATCO/PO BKL 98).

Onderzocht is of de werkzaamheden die in het VIR zijn beschreven zijn terug te vinden in de KL-methodieken. Hierbij is tevens gekeken naar overeenkomsten en verschillen in de methodieken.

Inhoud

1. Inleiding

'Bestuurs- en bedrijfsprocessen in moderne organisaties zijn in belangrijke mate afhankelijk van goed functionerende informatiesystemen. Veel processen zijn nagenoeg onmogelijk zonder de toepassing van geautomatiseerde gegevensverwerking. De genoemde afhankelijkheid wordt mede beïnvloed door de technologische ontwikkelingen op het gebied van de informatievoorziening' [1].

Door de steeds verdergaande technologische ontwikkelingen en het toepassen daarvan, neemt de behoefte aan informatiebeveiliging sterk toe. Het ministerie van binnenlandse zaken heeft op de behoefte aan informatiebeveiliging ingespeeld door het Voorschrift Informatiebeveiliging Rijksdienst (VIR) op te stellen. In dit voorschrift wordt rekening gehouden met de ontwikkelingen, op het gebied van informatietechnologie, "door geen gedetailleerde uitvoeringsregels te stellen, maar alleen op hoofdlijnen vast te leggen waaraan het informatiebeveiligingsbeleid moet voldoen" [2].

Aangezien het VIR van kracht is voor alle overheidsorganisaties dient ook de krijgsmacht een informatiebeveiligingsbeleid te voeren dat minimaal voldoet aan het VIR. Door de Beveiligings Autoriteit (BA) van het Ministerië van Defensie is het 'Beleidsdocument Informatiebeveiliging' [3] opgesteld. Dit beleidsdocument geeft aan hoe de waarborging van de betrouwbaarheid van de informatievoorziening bij en door het Ministerie van Defensie gerealiseerd moet worden. Waarbij met betrouwbaarheid het volgende bedoeld wordt: 'de mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening'.

Met als leidraad artikel 3 van het VIR wordt in het 'Beleidsdocument Informatiebeveiliging' een beleidskader aangegeven. Een van de werkzaamheden, die binnen het VIR beschreven wordt, is het op systematische wijze bepalen welk stelsel van beveiligingsmaatregelen getroffen dient te worden voor elk informatiesysteem en/of verantwoordelijkheidsgebied binnen een organisatie. De resultaten van deze werkzaamheden worden opgenomen in een Informatie Beveiligings Plan (IBP). Het VIR beschrijft een aantal activiteiten die uitgevoerd dienen te worden om tot een stelsel van beveiligingsmaatregelen te komen. Het betreft hier o.a. de zogenaamde afhankelijkheids- en kwetsbaarheidsanalyse. Deze activiteiten zullen in de volgende hoofdstukken nader uitgewerkt worden.

De Koninklijke Landmacht (KL) beschikt over een tweetal methodieken die gebruikt kunnen worden voor het bepalen van een stelsel van beveiligingsmaatregelen. Het betreft de KL-methodiek 'Handleiding voor het uitvoeren van het Informatiebeveiligingsproces' [4] en de 'KL-methodiek Integrale VeiligheidsZorg management' [5]. De 'Handleiding voor het uitvoeren van het Informatiebeveiligingsproces' is opgesteld door de sectie Commandovoering en Informatie Voorziening van de afdeling Beleidsontwikkeling van de Landmachtstaf

(LAS/BO/CIV), voorheen de sectie Commandovoering en Informatie Voorziening van de Directie Operatiën (DOKL/CIV). De 'KL-methodiek Integrale Veiligheids-Zorg management' is opgesteld door de Projectorganisatie Bewakingssysteem KL 98 van het NATionaal COmmando (NATCO/PO BKL 98).

1.1 Doel van het onderzoek

LAS/BO/CIV heeft TNO-FEL verzocht, binnen het kader van de 'Raamopdracht Informatiebeveiliging KL' (opdrachtnr. A94KL646), te onderzoeken of het tweetal KL-methodieken, voor wat betreft informatiebeveiliging, aansluit op het beleidskader en de daarbij uit te voeren werkzaamheden dat wordt geschetst door het beleidsdocument. Daar waar de methodieken niet aansluiten dienen aanvullende activiteiten uit andere methodieken of bronnen aangegeven te worden.

Daarnaast is door TNO-FEL een onderzoek verricht naar de toepasbaarheid van de in de 'Handleiding voor het uitvoeren van het Informatiebeveiligingsproces' opgenomen processen voor het bepalen van de feitelijke/vereiste beschikbaarheid, integriteit en vertrouwelijkheid van bedrijfsprocessen en/of informatiesystemen.

1.2 Indeling rapport

Om te beginnen zijn in hoofdstuk 2 beschrijvingen opgenomen van het Voorschrift Informatiebeveiliging Rijksdienst (VIR), van de KL-methodiek 'Handleiding voor het uitvoeren van het InformatieBeveiligings Proces' (HIBP) en van de 'KL-methodiek Integrale VeiligheidsZorg management' (IVZ-management). Tevens zijn in dit hoofdstuk de algemene overeenkomsten en verschillen van de methodieken opgenomen.

Vervolgens zijn de activiteiten afhankelijkheidsanalyse, het identificeren en analyseren van bedreigingen, de kwetsbaarheidsanalyse en het opstellen van het informatiebeveiligingsplan beschreven en zijn de relaties met de KL-methodieken aangegeven in respectievelijk hoofdstuk 3, 4, 5 en 6.

In hoofdstuk 7 zijn de aandachtspunten uitvoeringsvolgorde subprocessen HIBP, het beschikbaarheidsproces volgens het HIBP, het integriteitsproces volgens het HIBP en het vertrouwelijkheidsproces volgens het HIBP nader onderzocht.

Tot slot zijn in hoofdstuk 8 de conclusies en aanbevelingen op een rij gezet.

2. Beschrijving methodieken

Om een indruk te verkrijgen van de onderzochte methodieken worden in dit hoofdstuk de onderzochte methodieken globaal beschreven. Tevens wordt in dit hoofdstuk een algemene vergelijking van de methodieken gegeven.

2.1 Het Voorschrift Informatiebeveiliging Rijksdienst 'VIR'

In het Voorschrift Informatievoorziening Rijksdienst (VIR) is op hoofdlijnen vastgelegd waaraan het informatiebeveiligingsbeleid van de overheid moet voldoen. Daarnaast beschrijft het de aard van de activiteiten die uitgevoerd moeten worden tijdens het ontwikkel-, verwervings- en/of exploitatietraject van een informatiesysteem om tot een samenhangend geheel van veiligheidsmaatregelen te komen. Dit kunnen zowel technische, procedurele, personele, fysieke, als organisatorische maatregelen zijn.

Het VIR verstaat onder informatiebeveiliging 'het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van een informatiesysteem en daarmee van de informatie daarin'. Betrouwbaarheid heeft, binnen het VIR, betrekking op de 3 aspecten: beschikbaarheid, integriteit en exclusiviteit. Beschikbaarheid is de mate waarin een informatiesysteem in bedrijf is op het moment dat de organisatie het nodig heeft. Integriteit is de mate waarin een informatiesysteem zonder fouten is. Exclusiviteit is de mate waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden.

Om tot een betrouwbare informatievoorziening te komen, dient voor elk informatiesysteem en/of verantwoordelijkheidsgebied een viertal activiteiten plaats te vinden:

- vaststellen in hoeverre bestuurs- of bedrijfsprocessen die door informatiesystemen ondersteund worden, afhankelijk zijn van de betrouwbaarheid van deze systemen en vaststellen welke potentiële schades kunnen optreden als gevolg van het falen van deze informatiesystemen. Dit gebeurt door middel van een afhankelijkheidsanalyse. Voor de verdere uitwerking hiervan wordt verwezen naar het hoofdstuk afhankelijkheidsanalyse. De afhankelijkheidsanalyse mondt uit in een aan het informatiesysteem of verantwoordelijkheidsgebied te stellen verzameling van betrouwbaarheidseisen;
- identificeren en analyseren van bedreigingen;
- kiezen van beveiligingsmaatregelen, waarna door middel van een kwetsbaarheidsanalyse geverifiëerd kan worden dat aan de gestelde betrouwbaarheidseisen wordt voldaan;
- beschrijven van alle gekozen maatregelen in een informatiebeveiligingsplan. Het informatiebeveiligingsplan bevat een opsomming van alle beveiligings-

maatregelen en/of de vindplaatsen daarvan - inclusief een calamiteitenparagraaf - welke voor een informatiesysteem of een verantwoordelijkheidsgebied van kracht zijn. Het informatiebeveiligingsplan dient als basis voor het uitvoeren en het periodiek toetsen en evalueren van de geldigheid van de beschreven maatregelen. Indien nodig, worden de gekozen maatregelen aangepast aan nieuwe situaties of dreigingen.

2.2 Beschrijving KL-methodiek 'Handleiding voor het uitvoeren van het Informatiebeveiligingsproces'

De 'Handleiding voor het uitvoeren van het InformatiebeveiligingsProces' (verder te noemen als HIBP) beschrijft de in een stappenplan opgenomen activiteiten die uitgevoerd dienen te worden voor het opstellen van een Informatie Beveiligings Plan (IBP). Het IBP geeft het lijnmanagement (voor de KL is dit de commandant van een eenheid) inzicht in:

- het vereiste minimum van de informatiebeveiliging m.b.t. de te beveiligen belangen;
- de mate waarin de geautomatiseerde informatievoorziening voldoet aan dit vereiste minimum niveau;
- de organisatorische en technische beveiligingsmaatregelen om de geautomatiseerde informatievoorziening op het vereiste minimum niveau te brengen en te houden;
- datgene waartegen niet wordt beveiligd en de risico's wanneer bewust maatregelen achterwege worden gelaten;
- maatregelen om in geval van calamiteiten de informatievoorziening binnen de gestelde tijd weer functionerend te krijgen (calamiteitenplan);
- audit en control maatregelen voor het regelmatig toetsen en onderhouden van het informatiebeveiligingsplan.

De uit te voeren activiteiten (stappen) vormen samen het informatiebeveiligingsproces. Het proces is toepasbaar in: bestaande situaties, bij aanschaf van automatiseringsmiddelen en bij ontwikkeling van automatiseringsmiddelen en/of applicaties. Het proces is inzetbaar in vredestijd op de vredeslokatie en tijdens crisisbeheersingsoperaties op andere lokaties dan de vredeslokatie. De benadering van het proces vindt plaats vanuit de bedrijfsprocessen, automatiseringsmiddelen, omgevingsinvloeden en de beveiligingsaspecten beschikbaarheid, integriteit en vertrouwelijkheid.

Het informatiebeveiligingsproces is opgedeeld in subprocessen. Ieder subproces is een groepering van bij elkaar horende activiteiten (werkzaamheden). De volgende subprocessen zijn onderkend:

1. inventariseren bedrijfsprocessen en gegevens;
2. inventariseren automatiseringsmiddelen;
3. bepalen procesconfiguraties;
4. typeren bedrijfsprocessen;
5. bepalen beveiligingseisen en systeemconfiguraties;
6. bepalen feitelijke beveiligingsniveaus;
7. toetsen vereiste versus feitelijke beveiligingsniveaus;
8. uitvoeren kwetsbaarheidsanalyse;
9. formuleren maatregelen;
10. toetsen en vaststellen maatregelen;
11. opstellen en vaststellen informatiebeveiligingsplan;
12. goedkeuren informatiebeveiligingsplan;
13. uitvoeren informatiebeveiligingsplan.

De HIBP is onder andere gebaseerd op het 'Beleid Informatie Technologie' (BIT) en op de vigerende beveiligingsregelgeving, die is opgenomen in de Ministeriële Publicatie MP 10-10 deel 6 [6].

2.3 Beschrijving KL-regelgeving 'KL-methodiek Integrale VeiligheidsZorg management' (IVZ-management)

Onder Integrale VeiligheidsZorg management (IVZ-management) wordt bij de KL verstaan: 'het uitvoeren van alle management activiteiten op het gebied van bewaking en beveiliging (inbegrepen het handhaven van orde en rust), alsmede het uitvoeren van de management activiteiten binnen het raakvlakmanagement m.b.t. ARBO-zorg, milieuzorg, brandweerzorg en procescontrole (bewaken van 24-uurs bedrijfsprocessen)'. De KL-methodiek IVZ-management beschrijft hoe te komen tot het 'Veiligheidszorg Informatie Pakket' (VIP). Het VIP is een bundeling van plannen die voortvloeien uit de Integrale VeiligheidsZorg (IVZ). Deze plannen dienen te worden opgesteld door de verantwoordelijke commandant (lijnmanager). Het betreft de volgende plannen:

- het BasisPlan Integrale VeiligheidsZorg (BP-IVZ);
- het PLAN Interne Veiligheidszorg Organisatie (PLAN-IVO);
- het PLAN Externe Veiligheidszorg Organisatie (PLAN-EVO).

Het BP-IVZ geeft een overzicht van alle getroffen (beveiligings)maatregelen op basis van beleid, het risicoprofiel, de vitaliteit van de bedrijfsprocessen van "klanten", scenario's en verder van belang zijnde lokale/situationele omstandigheden. Het BP-IVZ regelt alle zaken en activiteiten die onder de normale routine vallen. Het BP-IVZ bestaat weer uit de volgende deelplannen:

- het VeiligHeidsZorg BeleidsPlan (VHZ-BP): dit plan verwoordt in hoofdlijnen het beleid van de verantwoordelijke commandant op het gebied van integrale veiligheidszorg;
- het Risico PROfiel (RIPRO): in het RIPRO wordt een totaalbeeld geschetst van de risico's die onderkend worden per object of lokatie;
- het Basis Veiligheidszorg Plan (BVP): in dit plan zijn de plattegronden van de betrokken objecten en lokatie opgenomen. Per object of lokatie wordt aangegeven of dit zich bevindt in vitaal gebied, beveiligd gebied of observatiegebied. Daarnaast wordt in dit plan een opsomming gegeven van alle organisatorische, bouwkundige en electronische (beveiligings)maatregelen per object of lokatie;
- het Informatie Beveiligings Plan (IBP): dit plan geeft een opsomming van alle beveiligingsmaatregelen die getroffen zijn voor de beveiliging van de informatiesystemen die zich binnen de objecten en/of lokaties bevinden;
- het BeWakings Plan (BWP): in dit plan worden o.a. de algemene instructies voor het bewakingspersoneel opgenomen;
- het Plan Ressort gebonden Taken (PRT): in dit plan zijn extra taken, bevoegdheden en verantwoordelijkheden van het IVZ-personeel opgenomen.

Het PLAN-IVO en het PLAN-EVO regelen de niet-routinematige zaken en activiteiten die zich bijvoorbeeld voordoen tijdens calamiteiten. Het PLAN-IVO beschrijft de berichtgeving en maatregelen die uitgevoerd dienen te worden door de IVZ-manager en/of het bewakingspersoneel op de plaats waar de calamiteit plaatsvindt. Het PLAN-EVO beschrijft deze zaken voor externe dienstverleners, zoals: Kmar, politie en/of brandweer.

3. Algemeen

In dit hoofdstuk worden de overeenkomsten en verschillen van algemene aard weergegeven.

3.1 Algemene overeenkomsten en verschillen

Het VIR is geschreven op een hoog abstractieniveau. De HIBP en de KL-methodiek IVZ management zijn praktisch ingesteld. De HIBP en de KL-methodiek IVZ management kunnen gezien worden als een praktische invulling van het VIR.

Voor alle methoden geldt dat de verantwoordelijkheid voor het uitvoeren van de activiteiten binnen deze methoden ligt bij het (lijn)management. Binnen de KL betekent dit dat de commandant van het betreffende onderdeel verantwoordelijk is voor het uitvoeren van deze activiteiten.

Het VIR en de 'Handleiding voor het uitvoeren van het Informatiebeveiligingsproces' (HIBP) beperken zich beide tot informatiebeveiliging. De KL-methodiek IVZ-management, daarentegen, is een methodiek die de werkzaamheden om te komen tot een adequate beveiliging, in de breedste zin van het woord, van een KL object, lokatie, eenheid of afdeling beschrijft. Deze methodiek gaat dus verder dan alleen informatiebeveiliging.

Het uitvoeren van de werkzaamheden en activiteiten beschreven in het VIR en de HIBP resulteren in een Informatie Beveiligings Plan (IBP). Het uitvoeren van de activiteiten en werkzaamheden van de KL-methodiek IVZ-management heeft een bundeling van plannen als resultaat. Eén van die plannen binnen deze bundeling is een IBP. Bij de beschrijving die IVZ-management geeft over het IBP worden de volgende documenten als onderhavige regelgeving beschouwd:

- Beleidsbundel Informatiebeveiliging KL;
- Handleiding voor het uitvoeren van het informatiebeveiligingsproces;
- concept MP 10-10 deel 6.

Uit de omschrijving, die door de KL-methodiek IVZ-management wordt gegeven met betrekking tot het IBP, kan worden opgemaakt dat de invulling van een IBP kan (dient te) worden uitgevoerd conform de HIBP. Voor het verloop van het onderzoek is dan ook aangenomen dat de KL-methodiek IVZ management voor het opstellen van een IBP verwijst naar de HIBP.

Het VIR en de HIBP gebruiken verschillende benamingen voor dezelfde begrippen. Daarnaast worden twee totaal verschillende begrippen van dezelfde naam voorzien. Het betreft het begrip 'betrouwbaarheidseisen' (VIR) en het begrip

'betrouwbaarheid of integriteit' (HIBP). Het VIR verstaat onder het begrip 'betrouwbaarheidseisen' de verzameling van exclusiviteitseisen, integriteitseisen en beschikbaarheidseisen, terwijl de HIBP spreekt over 'betrouwbaarheid' waarmee gedoeld wordt op integriteit. Om in de toekomst verwarringen te voorkomen wordt aanbevolen de begrippen in de HIBP te benoemen conform het VIR.

Het VIR geeft aan dat op beleidsniveau de informatiebeveiligingsaspecten geclassificeerd dienen te worden, maar geeft zelf geen classificering aan. Binnen de HIBP en de KL-methodiek IVZ-management worden de informatiebeveiligingsaspecten wel geclassificeerd.

De HIBP geeft een volgorde aan de subprocessen, waarbij wordt gesteld dat pas aan een volgend subproces kan worden begonnen wanneer de resultaten van het voorgaande subproces bekend zijn. Hierbij wordt de indruk gewekt dat de subprocessen ook daadwerkelijk in die volgorde uitgewerkt dienen te worden om tot een goed resultaat te komen. Het VIR geeft echter geen volgorde aan voor het uitvoeren van de afhankelijkheidsanalyse, kwetsbaarheidsanalyse en inventarisatie en analyse van de bedreigingen. Dit neemt niet weg dat eerst de betrouwbaarheidseisen (resultaat van de afhankelijkheidsanalyse), een inventarisatie en analyse van bedreigingen en de te treffen maatregelen bekend moeten zijn om een kwetsbaarheidsanalyse uit te kunnen voeren. Het VIR geeft echter geen volgorde aan voor het uitvoeren van een afhankelijkheidsanalyse en een inventarisatie en analyse van bedreigingen.

3.2 Specifieke overeenkomsten en verschillen

Om een beeld te krijgen van de specifieke overeenkomsten en verschillen tussen de genoemde methodieken zal in de volgende hoofdstukken verder ingegaan worden op de afhankelijkheidsanalyse, identificeren en analyseren van bedreigingen, de kwetsbaarheidsanalyse en het opstellen van het informatiebeveiligingsplan. Daarnaast zullen apart de processen voor het bepalen van de beschikbaarheid, integriteit en vertrouwelijkheid, zoals deze beschreven zijn in de HIBP, worden onderzocht op hanteerbaarheid en/of bruikbaarheid.

4. Afhankelijkheidsanalyse

In dit hoofdstuk wordt onderzocht of met behulp van een deel van de activiteiten van de HIBP een afhankelijkheidsanalyse volgens het VIR uitgevoerd kan worden. Voor de uitvoering van dit onderzoek zal een beschrijving worden gegeven van de afhankelijkheidsanalyse volgens het VIR. De stappen binnen de afhankelijkheidsanalyse zullen worden gerelateerd aan de corresponderende activiteiten uit de HIBP. Daar waar de HIBP niet toereikend is zullen activiteiten uit andere methodieken/bronnen worden aangegeven.

4.1 Beschrijving afhankelijkheidsanalyse volgens het VIR

De afhankelijkheidsanalyse bestaat uit een vijftal stappen. De eerste 3 stappen zijn gericht op het verkrijgen van inzicht in de mate waarin de bedrijfsprocessen afhankelijk zijn van het adequaat functioneren van het informatiesysteem. De laatste 2 stappen zijn gericht op het bepalen van een set van betrouwbaarheidseisen die aan het informatiesysteem worden gesteld. De stappen zijn achtereenvolgens:

- [A.1] inventariseren van de doelstellingen en de bestuurs- en bedrijfsprocessen. Hiermee wordt inzicht verkregen in de doelstellingen, producten en kerngegevens van de bestuurs- en bedrijfsprocessen, alsmede in de samenhang hiertussen en de relaties met externe instanties;
- [A.2] vaststellen van de relatie tussen de bestuurs- en bedrijfsprocessen en het informatiesysteem. Van belang is hierbij om te bepalen welke processen door het informatiesysteem worden ondersteund en op welke manier dat gebeurt. Ook de positieve effecten van informatiebeveiliging dienen te worden bepaald;
- [A.3] vaststellen van de mogelijke schade als gevolg van verstoringen in de informatievoorziening. De mogelijke schade bestaat uit directe, herstel- en vervolgschade. Directe schade is het verlies van activa, herstelschade bestaat uit de kosten die gemaakt moeten worden om de activa opnieuw aan te schaffen of op te bouwen en gevolgschade is alle indirecte schade die verbonden is met het voorgaande;
- [A.4] vaststellen van de maximaal toelaatbare schade. Bepalen welke schade geaccepteerd wordt door de organisatie;
- [A.5] formuleren van de aan het informatiesysteem te stellen eisen. Deze eisen worden opgesplitst in beschikbaarheids-, integriteits- en exclusiviteitseisen.

4.2 Relatie met de HIBP

De HIBP zal in relatie worden gebracht met de stappen van de afhankelijkheidsanalyse.

Door het uitvoeren van subproces 1 - Inventariseren bedrijfsprocessen en gegevens - van de HIBP kan stap [A.1] worden gerealiseerd.

Stap [A.2] kan worden verkregen door subproces 3 - Bepalen procesconfiguraties - van de HIBP uit te voeren. Subproces 3 maakt gebruik van de resultaten van de subprocessen 1 en 2. Met subproces 1 worden de bedrijfsprocessen geïnventariseerd. Binnen subproces 2 dienen de IT-middelen, en de daarbij behorende technische gegevens, geïnventariseerd te worden. Binnen de afhankelijkheidsanalyse wordt echter alleen gekeken naar de relatie tussen bedrijfsprocessen en informatiesystemen. Een informatiesysteem is opgebouwd uit een verzameling van IT-middelen. Omdat hier alleen informatiesystemen relevant zijn is het niet noodzakelijk om IT-middelen te inventariseren. Subproces 2 kan dus beperkt worden tot een inventarisatie van de informatiesystemen die nodig zijn voor de uitvoering van de bedrijfsprocessen. Er hoeft niet nader gespecificeerd te worden met welke IT-middelen dit gebeurd. Inventarisatie van de IT-middelen is echter wel noodzakelijk voor het bepalen van de beveiligingsmaatregelen, het analyseren van de bedreigingen en het uitvoeren van een kwetsbaarheidsanalyse.

Het VIR geeft aan dat binnen het informatiebeveiligingsbeleid een classificatie van de informatiebeveiligingsaspecten moet worden opgenomen. Deze classificatie dient gebruikt te worden bij de uitvoering van de stappen [A.3] en [A.4]. Deze stappen resulteren in een overzicht van de bedrijfsprocessen gerelateerd aan de classificaties van de informatiebeveiligingsaspecten. Het subproces 4 - Typeren bedrijfsprocessen - geeft voor de 3 informatiebeveiligingsaspecten een classificering aan. Het subproces geeft slechts een summiere indicatie van de schade bij de diverse classificeringen (zie bijlage B van de HIBP). In de Ministeriële Publicatie 10-10[1] (MP 10-10) wordt dit wel gedaan voor de classificering van de vertrouwelijkheid. Door uitvoering van subproces 4, in combinatie met de MP 10-10, kan per bedrijfsproces uitsluitend voor het informatiebeveiligingsaspect vertrouwelijkheid de mogelijke schade en de maximaal toelaatbare schade worden bepaald.

Samen met de resultaten van de subprocessen 1 t/m 4 kan door uitvoering van subproces 5 - Bepalen beveiligingseisen en systeemconfiguraties - de stap [A.5] van de afhankelijkheidsanalyse worden uitgevoerd.

4.3 Relatie met de KL-methodiek IVZ-management

Ook de KL-methodiek IVZ-management zal in relatie worden gebracht met de stappen van de afhankelijkheidsanalyse.

---

1 In de Ministeriele Publicatie, MP 10-10, staat onder andere vermeld wat voor soort schade, en in welke mate, er kan ontstaan wanneer gerubriceerde informatie verloren gaat of in verkeerde handen terecht komt.

Binnen het IVZ-management wordt gestreeft naar het opstellen van een bundeling van plannen. Eén van deze plannen is het Informatie Beveiligings Plan (IBP). Bij de beschrijving die de KL-methodiek geeft over het IBP worden de volgende documenten als onderhavige regelgeving beschouwd:

- Beleidsbundel Informatiebeveiliging KL;
- Handleiding voor het uitvoeren van het informatiebeveiligingsproces;
- concept MP 10-10 deel 6.

Hiervan uitgaande kan worden verondersteld dat voor het uitvoeren van een afhankelijkheidsanalyse wordt verwezen naar de subprocessen 1 t/m 5 van het document 'Handleiding voor het uitvoeren van het Informatiebeveiligingsproces'.

Het IVZ-management biedt echter een aantal extra hulpmiddelen om een afhankelijkheidsanalyse uit te voeren. De KL-methodiek IVZ-management geeft een praktisch bruikbare mate van schade aan de classificeringen van de informatiebeveiligingsaspecten. De 'handleiding voor het uitvoeren van het Informatiebeveiligingsproces' geeft slechts een theoretische mate van schade aan. Door de twee methodieken te combineren is het mogelijk een beter inzicht te krijgen in de mate van schade. Het bepalen van de mate van schade wordt beschreven in het deel dat betrekking heeft op het Risico PROfiel (RIPRO). Deze hulpmiddelen hebben betrekking op de stappen A.3 en A.4 van de afhankelijkheidsanalyse.

De overige activiteiten die door de KL-methodiek IVZ-management worden voorgeschreven hebben geen relatie tot de afhankelijkheidsanalyse, zoals deze door het VIR wordt voorgeschreven.

4.4 Conclusies en aanbevelingen

In tabel 4.1 wordt een overzicht gegeven van de te volgen subprocessen voor het uitvoeren van een afhankelijkheidsanalyse.

Subproces 1 kan zonder meer worden uitgevoerd voor het realiseren van stap [A.1].

Voor stap [A.2] is een beperkte uitvoering van subproces 2 gecombineerd met het uitvoeren van subproces 3 voldoende. Hierbij dient subproces 2 beperkt te worden tot het inventariseren van de informatiesystemen. Aanbevolen wordt om de inventarisatie van de IT-middelen binnen de afhankelijkheidsanalyse uit te voeren. Op deze manier is het mogelijk een beter inzicht te krijgen in het soort bedreigingen en de te nemen maatregelen.

Subproces 4 van de HIBP biedt een voldoende classificering van de informatiebeveiligingsaspecten. Aangevuld met de KL-methodiek IVZ-management en de MP 10-10 resulteert dit subproces in de vaststelling van de mogelijke schade en de

maximaal toelaatbare schade. Dit komt overeen met het uitvoeren van de stappen [A.3] en [A.4] van de afhankelijkheidsanalyse.

Subproces 5 kan worden uitgevoerd voor het realiseren van stap [A.5].

Tabel 4.1: Overzicht van de resultaten van de vergelijking tussen de afhankelijkheidsanalyse van het VIR en de HIBP.

stappen afh. analyse volgens VIR	subprocessen HIBP	Aanvullende handelingen op de subprocessen HIBP
A.1 inventariseren bedrijfsprocessen	subproces 1 - Inventariseren bedrijfsprocessen en gegevens	n.v.t.
A.2 vaststellen relaties	subproces 2 (beperkt) - Inventariseren automatiseringsmiddelen + subproces 3 - Bepalen procesconfiguraties	n.v.t.
A.3 vaststellen mogelijke schade	subproces 4 - Typeren bedrijfsprocessen	bepalen mogelijke schade voor de beveiligingsaspecten exclusiviteit, integriteit en beschikbaarheid[2]
A.4 vaststellen van de maximaal toelaatbare schade	subproces 4	bepalen maximaal toelaatbare schade voor de beveiligingsaspecten exclusiviteit, integriteit en beschikbaarheid[3]
A.5 formuleren eisen	subproces 5 - Bepalen beveiligingseisen en systeemconfiguraties	n.v.t.

2 Hiervoor kan gebruik gemaakt worden van de waarde-incident tabel en de INCIDETAR methodiek die zijn beschreven in de KL-methodiek IVZ management. Voor het aspect exclusiviteit kan tevens gebruik gemaakt worden van de MP 10-10 deel 3. Exclusiviteit wordt binnen de MP 10-10 aangegeven als vertrouwelijkheid.

3 Zie voetnoot 2

5. Identificeren en analyseren van bedreigingen

In dit hoofdstuk wordt onderzocht met welk deel van de activiteiten van de HIBP het identificeren en analyseren van bedreigingen uitgevoerd kan worden. Het identificeren en analyseren van bedreigingen wordt gerelateerd aan de juiste activiteiten uit de HIBP.

5.1 Beschrijving identificeren en analyseren van bedreigingen volgens het VIR

Om gericht beveiligingsmaatregelen te kunnen treffen, is het nodig inzicht te krijgen in de factoren die de gestelde betrouwbaarheidseisen bedreigen. Om een zo volledig mogelijk beeld te krijgen van alle mogelijke bedreigingen, moet voor alle componenten van een informatiesysteem worden nagegaan waardoor verlies aan beschikbaarheid, integriteit en exclusiviteit kan ontstaan. Als bekend is op welke manier bedreigingen tot verstoringen leiden, kunnen incidenten worden geconstrueerd. De beschrijvingen van deze incidenten zijn nodig om in de volgende fase de juiste maatregelen te kunnen treffen.

5.2 Relatie met de HIBP

Identificeren en analyseren van bedreigingen kan worden gerealiseerd door de uitvoering van subproces 8 - Uitvoeren kwetsbaarheidsanalyse.

5.3 Relatie met de KL-methodiek IVZ-management

Ook hier kan worden verwezen naar de subprocessen van de HIBP die uitgevoerd dienen te worden voor het identificeren en analyseren van de bedreigingen. Uit de vorige paragraaf is duidelijk geworden dat voor het identificeren en analyseren van de bedreigingen subproces 8 dient te worden uitgevoerd.

Bij de KL-methodiek IVZ-management wordt binnen het Risico PROfiel (RIPRO) een totaalbeeld geschetst van de risico's waaraan een object of lokatie blootgesteld kan worden. Hierbij dient gedacht te worden aan potentiële incidenten en mogelijke scenario's. Tevens bevat dit plan een profiel van mogelijke individuen en/of organisaties die de oorzaak kunnen zijn van mogelijke incidenten. Het betreft hier zogenaamde daderprofiel.

Wanneer de KL-methodiek IVZ-management wordt uitgevoerd dient bij het opstellen van het IBP rekening gehouden te worden met de potentiële incidenten, scenario's en daderprofielen die zijn opgenomen in het RIPRO. Deze incidenten,

scenario's en daderprofielen hebben betrekking op alle mogelijke zaken die beveiligd dienen te worden. Binnen het IBP zullen alleen die gegevens worden opgenomen die betrekking hebben op informatiesystemen. Een deelverzameling van de potentiële incidenten, scenario's en het daderprofiel uit dit RIPRO kunnen worden opgenomen in het IBP. Het betreft hier de gegevens die betrekking hebben op informatiesystemen of die door een vertaalslag kunnen worden aangepast, zodat ze betrekking hebben op informatiesystemen.

5.4 Conclusies en aanbevelingen

Tabel 5.1: Overzicht van de resultaten van de vergelijking van het identificeren en analyseren van bedreigingen volgens het VIR en de HIBP.

activiteiten VIR	subprocessen HIBP	Aanvullende handelingen op de subprocessen HIBP
identificeren en analyseren van bedreigingen	subproces 8 - Uitvoeren kwetsbaarheidsanalyse	RIPRO IVZ-management

Subproces 8 dient uitgevoerd te worden voor het identificeren en analyseren van bedreigingen.

Volgens de HIBP is het doel van subproces 8 het uitvoeren van de kwetsbaarheidsanalyse. Het subproces heet dan ook 'Uitvoeren kwetsbaarheidsanalyse'. Het VIR verstaat echter iets anders onder het uitvoeren van een kwetsbaarheidsanalyse, zie hiervoor het volgende hoofdstuk. Om spraakverwarringen te voorkomen wordt aanbevolen de naam van subproces 8 aan te passen aan de activiteiten die binnen dit subproces worden uitgevoerd. Wanneer de terminologie van het VIR wordt overgenomen kan subproces 8 benoemd worden als 'Identificeren en analyseren van bedreigingen'.

6. Kwetsbaarheidsanalyse

In dit hoofdstuk wordt onderzocht of met behulp van een deel van de activiteiten van de HIBP een kwetsbaarheidsanalyse volgens het VIR uitgevoerd kan worden. Voor de uitvoering van dit onderzoek zal een beschrijving worden gegeven van de kwetsbaarheidsanalyse volgens het VIR. De stappen binnen de kwetsbaarheidsanalyse zullen worden gerelateerd aan de juiste activiteiten uit de HIBP.

6.1 Beschrijving kwetsbaarheidsanalyse volgens het VIR

Uitgaande van de betrouwbaarheidseisen en de geïdentificeerde bedreigingen wordt een pakket van informatiebeveiligingsmaatregelen gekozen, waarbij het de voorkeur heeft om zoveel mogelijk gebruik te maken van maatregelen die binnen de organisatie al uit andere hoofde zijn getroffen. De kosten van de gekozen maatregelen dienen in evenwicht te zijn met de baten, dus met de beperking van de mogelijke schade. Het gekozen stelsel van maatregelen dient bovendien op elk moment van dien aard te zijn dat aantoonbaar aan de betrouwbaarheidseisen wordt voldaan. Hiertoe zal periodiek een kwetsbaarheidsanalyse moeten worden uitgevoerd. Op basis van de kwetsbaarheidsanalyse kan worden geconstateerd of de resulterende betrouwbaarheid van het systeem (nog) voldoet aan de gestelde eisen. Als dit niet het geval is, dienen andere of aanvullende maatregelen genomen te worden en moet de kwetsbaarheidsanalyse opnieuw worden uitgevoerd. Binnen deze analyse wordt tevens nagegaan welke risico's (verstoringen in het bedrijfsproces, door toedoen van bedreigingen) geaccepteerd worden en welke niet. Als het systeem voldoende betrouwbaar is bevonden, worden de beveiligingsmaatregelen uitgewerkt en opgenomen in een informatiebeveiligingsplan. Het opstellen van het informatiebeveiligingsplan valt buiten de grenzen van de kwetsbaarheidsanalyse.

6.2 Relatie met de HIBP

Door het uitvoeren van de subprocessen 6, 7, 9 en 10 kan een kwetsbaarheidsanalyse volgens het VIR worden uitgevoerd. Binnen deze processen wordt het feitelijke beveiligingsniveau vergeleken met het vereiste (gewenste) beveiligingsniveau. Wanneer het vereiste niveau hoger is dan het feitelijke niveau dienen, binnen subproces 9, maatregelen getroffen te worden. Deze maatregelen dienen ervoor te zorgen dat het feitelijke niveau gelijk getrokken wordt met het vereiste niveau. De te treffen maatregelen worden getoetst op aspecten als doeltreffendheid, onderhoudbaarheid, realiseerbaarheid. Tevens wordt onderzocht of de kosten van de te treffen maatregelen in verhouding zijn met de mogelijke schade die kan worden opgelopen.

6.3 Relatie met de KL-methodiek IVZ-management

Ook hier kan worden verwezen naar de subprocessen van de HIBP die uitgevoerd dienen te worden voor het uitvoeren van een kwetsbaarheidsanalyse. De vorige paragraaf geeft aan dat het de subprocessen 6, 7, 9 en 10 betreft.

De KL-methodiek IVZ-management heeft binnen het opstellen van het RIPRO een tweetal methodieken aan waarmee een kwetsbaarheidsanalyse kan worden uitgevoerd. Het betreft de volgende methodieken:

- de waarde-incident-matrix;
- de INCI-DETAR-methodiek.

Deze methodieken zijn gericht op het analyseren van Organisatorische, Bouwkundige en Electronische maatregelen (de zogenaamde OBE-maatregelen). De OBE-maatregelen, zoals ze binnen het RIPRO behandeld worden, zijn sterk gericht op organisatorische en fysieke beveiliging. Het is echter mogelijk deze methodieken toe te passen bij het uitvoeren van een kwetsbaarheidsanalyse met betrekking tot informatiesystemen.

6.4 Conclusies en aanbevelingen

Tabel 6.1: Overzicht van de resultaten van de vergelijking tussen de kwetsbaarheidsanalyse van het VIR en de HIBP.

activiteiten VIR	subprocessen HIBP	Aanvullende handelingen op de subprocessen HIBP
kwetsbaar-heidsanalyse	subprocessen 6 - Bepalen feitelijke beveiligingsniveaus, 7 - Toetsen vereiste versus feitelijke beveiligingsniveaus, 9 - Formuleren maatregelen en 10 - Toetsen en vaststellen maatregelen	RIPRO IVZ-management/waarde-incident-matrix, INCI-DETAR-methodiek

Met behulp van de HIBP is het mogelijk, zonder aanvullende handelingen, een kwetsbaarheidsanalyse uit te voeren.

Het is aan te bevelen de subprocessen van de HIBP samen te voegen en te hernoemen tot kwetsbaarheidsanalyse, vanwege de uniformiteit met het VIR.

7. Opstellen van het 'Informatie Beveiligings Plan (IBP)'

In dit hoofdstuk wordt onderzocht of met behulp van een deel van de activiteiten van de HIBP een Informatie Beveiligings Plan (IBP) kan worden opgesteld dat voldoet aan de normen gesteld in het VIR. Voor de uitvoering van dit onderzoek zal een beschrijving worden gegeven van het IBP volgens het VIR. De vereiste onderdelen van het IBP zullen worden vergeleken met het IBP uit de HIBP.

7.1 Beschrijving IBP volgens het VIR

In het VIR staat beschreven dat voor elk informatiesysteem en voor elk verantwoordelijkheidsgebied een IBP dient te worden opgesteld. Het VIR geeft als definitie voor een IBP: opsomming van alle beveiligingsmaatregelen en/of vindplaatsen daarvan welke voor een informatiesysteem of een verantwoordelijkheidsgebied van kracht zijn.

Volgens het VIR is het doel van het IBP:
- dienen als communicatiemiddel richting gebruikers en technische staf;
- afleggen van verantwoording naar het hogere lijnmanagement;
- vormen van een basis voor periodieke controle.

Het IBP dient een beschrijving van het stelsel van te bevatten of minimaal een compleet stelsel van verwijzingen naar de plaatsen waar deze maatregelen zijn beschreven. De overweging waardoor tot deze maatregelen is gekomen hoeven niet in het IBP te worden opgenomen. Het VIR geeft aan dat de resultaten van de afhankelijkheids-, bedreigingen- en kwetsbaarheidsanalyse dienen te worden opgenomen in aparte bij de analyse behorende documenten. Daarnaast dient in het IBP tot uitdrukking te komen welke relaties er zijn ten opzichte van maatregelen die getroffen zijn voor andere verantwoordelijkheidsgebieden (voor zover van belang).

Hoewel de implementatie van het IBP ervoor zorgt dat de meeste bedreigingen niet tot onacceptabele schadelijke effecten leiden, moet er toch rekening mee worden gehouden dat er zich situaties kunnen voordoen waartegen het informatiesysteem niet bestand is. Daarom dient het IBP een calamiteitenparagraaf te bevatten waarin is vastgelegd op welke wijze belangrijke bestuurs- en bedrijfsprocessen worden voortgezet nadat een deel van het systeem uitvalt of onbruikbaar wordt. De calamiteitenparagraaf heeft het karakter van een draaiboek zodat in noodsituaties iedereen weet hoe te handelen.

Het IBP dient te worden goedgekeurd door de verantwoordelijke lijnmanager. Hierbij dient te worden vastgesteld dat het plan past binnen de uitgangspunten en randvoorwaarden van het informatiebeveiligingsbeleid.

Binnen een IBP dient er een actieplan te worden opgesteld (of een verwijzing naar dit actieplan te worden gegeven), waarin wordt aangegeven op welke termijn, met welke middelen en met welke menskracht de in het IBP opgenomen maatregelen (nieuwe dan wel stringentere maatregelen, die niet uit ander hoofde reeds van kracht zijn) zullen worden geïmplementeerd.

Het IBP dient periodiek te worden geëvalueerd om na te gaan of het hele pakket van maatregelen nog steeds voldoet aan de gewenste betrouwbaarheid en of het pakket van maatregelen goed wordt uitgevoerd. Een dergelijke evaluatie dient volgens een vastgesteld schema te worden uitgevoerd. Dit schema of minimaal een verwijzing naar het document waarin dit schema is beschreven dient te worden opgenomen in het IBP.

7.2 Relatie met de HIBP

Voor het opstellen van een IBP kan binnen de HIBP verwezen worden naar de subprocessen 11 en 12, 'Opstellen en vaststellen informatiebeveiligingsplan' respectievelijk 'Goedkeuren informatiebeveiligingsplan'.

Binnen subproces 11 zijn 4 stappen onderkend. Deze stappen zijn:
- stap 11.1 registreren resultaten informatiebeveiligingsproces;
- stap 11.2 formuleren audit en control maatregelen;
- stap 11.3 opstellen implementatieplan;
- stap 11.4 vaststellen informatiebeveiligingsplan.

In stap 11.1 wordt het IBP samengesteld op basis van de resultaten van de doorlopen subprocessen. In de voorgaande hoofdstukken is aangetoond dat de doorlopen subprocessen grote overeenkomsten hebben met de afhankelijkheids-, bedreigingen- en kwetsbaarheidsanalyse. Het VIR geeft aan dat de resultaten van deze analyses niet in het IBP maar in aparte bij de analyses behorende documenten dienen te worden opgenomen. Uit de doorlopen subprocessen zijn alleen de maatregelen die getroffen dienen te worden of de verwijzingen waar deze maatregelen beschreven staan voldoende voor het opstellen van een IBP conform het VIR.

In stap 11.2 wordt het IBP aangevuld met de audit en control maatregelen die nodig zijn voor de evaluatie, het onderhoud en het bewaken van de goede uitvoering van het IBP. Binnen het VIR wordt aangegeven dat dergelijke maatregelen opgenomen dienen te worden in het IBP of minimaal de verwijzing naar het document waar deze maatregelen opgenomen zijn.

Binnen stap 11.3 wordt een tijdsplan opgesteld voor de implementatie van de beveiligingsmaatregelen. In het VIR wordt een dergelijk tijdsplan aangeduid met actieplan. Ook voor dit actieplan, of de verwijzing naar een document waarin dit actieplan is beschreven, geldt dat dit opgenomen dient te zijn in het IBP.

Binnen stap 11.4 wordt het IBP vastgesteld door de verantwoordelijke lijnmanager, in dit geval de (onderdeels)commandant. Bij het vaststellen dient onder andere gecontroleerd te worden of het plan aansluit bij het informatiebeveiligingsbeleid. Ook in subproces 12 wordt het IBP vastgesteld. Het verschil met stap 11.4 van subproces 11 is dat het IBP nu goedgekeurd wordt door een naast hoger niveau binnen de organisatie dat verantwoordelijk is voor de realisatie van het informatiebeveiligingsbeleid. Het VIR spreekt alleen over goedkeuring van het IBP door de verantwoordelijke lijnmanager.

7.3 Relatie met de KL-methodiek IVZ-management

Voor het opstellen van een IBP wordt door KL-methodiek IVZ-management verwezen naar de HIBP of de MP 10-10. De methodiek heeft verder geen aanvullende activiteiten en/of werkzaamheden aangegeven.

7.4 Conclusies en aanbevelingen

Tabel 7.1: Overzicht van de resultaten van de vergelijking tussen het Informatie Beveiligings Plan van het VIR en de HIBP.

activiteiten VIR	subprocessen HIBP	Aanvullende handelingen op de subprocessen HIBP
opstellen en vaststellen IBP	subprocessen 11 - Opstellen en vaststellen informatiebeveiligingsplan en 12 - goedkeuren informatiebeveiligingsplan	n.v.t.

Voor het opstellen en vaststellen van het IBP kunnen de subprocessen 11 en 12 van de HIBP gebruikt worden. Voor het opstellen van een IBP conform het VIR is het echter niet nodig de resultaten van alle subprocessen in het IBP op te nemen. Voor stap 11.1 van subproces 11 geldt dat alleen de maatregelen die uit de subprocessen voortvloeien dienen te worden opgenomen (of een verwijzing naar waar deze maatregelen zijn opgenomen). In subproces 9 van de HIBP dienen de te treffen maatregelen geformuleerd te worden. Ook het calamiteitenplan dient binnen subproces 9 opgesteld te worden, zie hiervoor ook het vorige hoofdstuk.

De stappen 11.2 en 11.3 dienen te worden uitgevoerd voor het verkrijgen van een volledig IBP.

Volgens het VIR is stap 11.4 voldoende om een IBP vastgesteld te krijgen. Bij de verwerking van gerubriceerde informatie schrijft het informatiebeveiligingsbeleid van het Ministerie van Defensie echter voor dat een (informatie)systeem dient te worden goedgekeurd door de Beveiligings Autoriteit en/of de beveiligingscoördi-

nator KL. Hetzelfde geldt voor de bij het (informatie)systeem behorende documentatie (waaronder het IBP).

8. Overige aandachtspunten voor de HIBP

In dit hoofdstuk wordt tot slot gekeken naar de toepasbaarheid en gebruikersvriendelijkheid van de processen voor het bepalen van de (feitelijke/vereiste) beschikbaarheid, integriteit en vertrouwelijkheid bekeken op.

8.1 Evaluatie van het proces 'bepalen feitelijke/vereiste beschikbaarheid'

De HIBP geeft over het informatiebeveiligingsaspect beschikbaarheid de volgende toelichting. Stagnatie van een bedrijfsproces heeft nadelige gevolgen voor de slagkracht en de interne bedrijfsvoering van het Ministerie van Defensie/de Krijgsmacht/de organisatorische eenheid. Tevens kan een stagnatie economische schade tot gevolg hebben voor de betreffende organisatie.

Stagnatie van bedrijfsprocessen kan worden veroorzaakt door het ontbreken van benodigde gegevens die binnen de bedrijfsprocessen dienen te worden verwerkt. Wanneer de schade die hierdoor wordt opgelopen ontoelaatbaar groot wordt heeft de stagnatie zijn maximaal toelaatbare duur bereikt. Deze maximaal toelaatbare stagnatieduur bepaalt welke eisen aan een informatiesysteem gesteld dienen te worden. De maximaal toelaatbare stagnatieduur is de periode vanaf het ontstaan van de stagnatie tot aan het moment dat de schade die wordt opgelopen ontoelaatbaar wordt. De maximaal toelaatbare stagnatieduur bepaald de vereiste beschikbaarheid van een bedrijfsproces en dus ook voor de informatiesystemen die dit bedrijfsproces ondersteunen. Een eventuele stagnatie kan het gevolg zijn van:

- het niet beschikbaar zijn van apparatuur;
- het niet beschikbaar zijn van programmatuur;
- (over)belasting van het systeem.

De beschikbaarheid van een (informatie)systeem kan geclassificeerd worden. Binnen de HIBP is deze classificatie als volgt:

- absolute beschikbaarheid;
- zeer hoge beschikbaarheid;
- hoge beschikbaarheid;
- middelhoge beschikbaarheid;
- lage beschikbaarheid.

Om te kunnen bepalen of (aanvullende) maatregelen getroffen dienen te worden dient de feitelijke beschikbaarheid van de systeemconfiguratie bepaald te worden. Vergelijking van de vereiste beschikbaarheid met de feitelijke beschikbaarheid moet uitwijzen of (aanvullende) maatregelen nodig zijn.

8.1.1 Procesbeschrijving 'bepalen vereiste beschikbaarheid'

Het bepalen van de vereiste beschikbaarheid wordt primair door de eigenaar van het bedrijfsproces bepaald. De vereiste beschikbaarheid dient bepaald te worden door [4]:

- de tijd die nodig is voor het uitvoeren van het meest kritische proces binnen een missie;
- de maximaal toegestane stagnatieduur van het meest kritische proces.

De vereiste beschikbaarheid wordt berekend door de tijd die nodig is voor het uitvoeren van het meest kritische proces te delen door de som van de tijd die nodig is voor het uitvoeren van het meest kritische proces en de maximaal toelaatbare stagnatieduur. Door het nu verkregen getal te vermenigvuldigen met 100% wordt de vereiste beschikbaarheid weergegeven in procenten.

8.1.2 Procesbeschrijving 'bepalen feitelijke beschikbaarheid'

De feitelijke beschikbaarheid kan op twee manieren worden bepaald [4]:

- uit de praktijk opgedane ervaring met betrekking tot een bestaande systeemconfiguratie;
- door het uitvoeren van berekeningen met specificaties van de gebruikte automatiseringsmiddelen, zoals:
  - de onderlinge relaties tussen de automatiseringsmiddelen;
  - gegevens over de automatiseringsmiddelen zelf (Mean Time Between Failure - MTBF, Mean Time To Restore - MTTR);
  - gegevens over het vereiste onderhoud van deze automatiseringsmiddelen.

Helpdeskfunctionarissen en/of systeembeheerders weten vaak uit ervaring en hun technische kennis wat de beschikbaarheid van bepaalde informatiesystemen is. Wanneer deze kennis en ervaring aanwezig is, is het raadzaam de feitelijke beschikbaarheid te laten bepalen door deze functionarissen.

Het berekenen van de feitelijke beschikbaarheid gaat als volgt te werk. In de eerste plaats dient de systeemconfiguratie in kaart gebracht te worden. Hierbij is het mogelijk dat systeemcomponenten in serie of parallel geschakeld zijn. Met systeemcomponenten kunnen zowel hardware als software componenten bedoeld worden. Ook kunnen hier operators, die belangrijk zijn voor het goed functioneren van het informatiesysteem, mee worden bedoeld. Per systeemcomponent dient de feitelijke beschikbaarheid bepaald te worden. Er dient begonnen te worden met het berekenen van de feitelijke beschikbaarheid van de eventueel parallel geschakelde systeemdelen. De totale feitelijke beschikbaarheid van deze parallelle systeemdelen kan dan weer gezien worden als de feitelijke beschikbaarheid van een in serie geschakeld systeemdeel.

Als uitgangspunt wordt verondersteld dat parallel schakelen van systeemcomponenten alleen mogelijk is met identieke systeemcomponenten. Tevens kunnen er twee mogelijke vormen van parallel schakelen voorkomen. De eerste is de zoge-

naamde stand-by schakeling. Dit wil zeggen als een van de systeemdelen uitvalt wordt het andere systeemdeel actief. De tweede mogelijkheid van parallel schakelen is de daadwerkelijke parallel schakeling. Alle parallel geschakelde systeemdelen zijn in deze situatie actief.

Naast deze mogelijkheden van schakelen wordt er ook onderscheid gemaakt tussen enkelvoudige reparatie en meervoudige reparatie. Bij enkelvoudige reparatie wordt een eventueel defect systeemdeel pas gerepareerd wanneer alle parallel geschakelde systeemdelen defect zijn. Bij de meervoudige reparatie wordt een defect systeemdeel zo spoedig mogelijk gerepareerd.

Voor al deze situaties is in de HIBP een tabel opgenomen, waarin formules zijn opgenomen voor het berekenen van de feitelijke beschikbaarheid. De tabel bevat formules voor het berekenen van de feitelijke beschikbaarheid voor parallel schakelingen met maximaal 3 systeemdelen.

De formules die in deze tabel zijn opgenomen zijn gebaseerd op de Mean Time Between Failure (MTBF) en de Mean Time To Restore (MTTR) van de systeemdelen. Er wordt echter verondersteld dat deze waarden voor alle parallel geschakelde systemen gelijk zijn.

De feitelijke beschikbaarheid van de in serie geschakelde systemen wordt uiteindelijk berekend door de feitelijke beschikbaarheid van de afzonderlijke systeemdelen met elkaar te vermenigvuldigen.

8.1.3 Conclusies

De delen van de HIBP waarin het bepalen van de vereiste en de feitelijke beschikbaarheid wordt beschreven zijn verwarrend. Daarnaast bevatten deze delen veel informatie die voor het bereiken van de uiteindelijke doelen niet relevant is.

De vragenlijsten die zijn opgenomen zijn duidelijk, maar veel van de informatie die met behulp van deze lijsten wordt vergaard wordt niet gebruikt bij het bepalen van de vereiste en feitelijke beschikbaarheid.

Een vaak gehoorde klacht met betrekking tot de HIBP zijn de formules die zijn opgenomen binnen de procesbeschrijving 'bepalen feitelijke beschikbaarheid. Deze formules zouden te ingewikkeld zijn en daardoor voor veel functionarissen niet te hanteren zijn.

Tot slot kan opgemerkt worden of het zinvol is de beschikbaarheid van een (deel)systeem te berekenen. Een pragmatische oplossing kan worden gerealiseerd door de klassen van beschikbaarheid (van lage beschikbaarheid tot absolute beschikbaarheid) te koppelen aan een verzameling van maatregelen. Door te onderzoeken welke maatregelen binnen een (deel)systeem zijn uitgevoerd kan dan de

feitelijke beschikbaarheid bepaald worden. Als maatregelen kunnen gebruikt worden:

- het standby schakelen van (deel)systemen;
- het parallel schakelen van (deel)systemen;
- het dubbel afsteunen van (deel)systemen.

8.1.4 Aanbevelingen

Aanbevolen wordt de procesbeschrijving 'Bepalen vereiste beschikbaarheid' te beperken tot:

- een inleiding van het begrip vereiste beschikbaarheid met daarin opgenomen de tijdbalk m.b.t. de missie tijd. Waarbij moet worden opgemerkt dat de formule voor het bepalen van de vereiste beschikbaarheid verplaatst dient te worden naar het einde van de inleiding;
- het opnemen van vragen met betrekking tot:
  - het bepalen van het kritische proces;
  - het bepalen van de doorlooptijd van het kritische proces;
  - het bepalen van de gebruikstijden van het kritische proces, waaronder de operationele gebruikstijd en de niet-operationele gebruikstijd;
  - het bepalen van de maximaal toelaatbare stagnatieduur van het kritische proces;

De maatregelen die in deze procesbeschrijving zijn beschreven kunnen worden opgenomen in een apart hoofdstuk van deze bijlage of in een aparte bijlage van de HIBP. Dit omdat bij het bepalen van de vereiste beschikbaarheid nog geen sprake is van het nemen van maatregelen.

De vragen, die zijn opgenomen in de procesbeschrijving 'bepalen vereiste beschikbaarheid', met betrekking tot onderhoud en herstel opnemen bij de procesbeschrijving 'bepalen feitelijke beschikbaarheid'. Deze vragen hebben namelijk te maken met het bepalen van de MTTR van de systeemdelen.

De tabel waarin de formules voor het bepalen van de feitelijke beschikbaarheid van parallelle systeemdelen zijn opgenomen dient te worden aangepast. Voorgesteld wordt de in de tabel opgenomen uitwerkingen te verwijderen om verwarringen te voorkomen.

Aanbevolen wordt de formules te verwerken in een stukje programmatuur die de berekeningen voor het bepalen van de feitelijke beschikbaarheid kan uitvoeren. Door gebruik te maken van een gebruikersvriendelijke interface wordt het bepalen van de feitelijke beschikbaarheid aanzienlijk vereenvoudigd. Ook kunnen de formules verwerkt worden in een matrix, waarbij de beschikbaarheid is berekend voor verschillende MTBF en MTTR. Hierdoor wordt het mogelijk dat een gebruiker de beschikbaarheid van een parallel (deel)systeem kan aflezen voor gegeven MTBF en MTTR. Zijn de gegeven MTBF en MTTR niet in de tabel opgenomen

dan kan de gebruiker met behulp van interpoleren of extrapoleren de beschikbaarheid van het betreffende (deel)systeem benaderen.

Het rekenvoorbeeld dat is opgenomen binnen deze procesbeschrijving is goed bruikbaar. Door echter de uitwerking nog overzichtelijker te presenteren wordt het hanteren van de HIBP voor betrokken functionarissen vergemakkelijkt. Het toevoegen van meerdere rekenvoorbeelden versterkt de hanteerbaarheid van de HIBP ook aanzienlijk.

8.2 Evaluatie van het proces 'bepalen feitelijke/vereiste integriteit'

De HIBP geeft over het informatiebeveiligingsaspect integriteit de volgende toelichting. Integriteit (betrouwbaarheid) is de mate waarin de geproduceerde gegevens een correcte weergave zijn van de afgebeelde werkelijkheid en niets ten onrechte is toegevoegd, achtergehouden of verdwenen. Bij het bepalen van de afhankelijkheden van de bedrijfsprocessen is niet het achterhalen van het vereiste niveau van integriteit het streven, maar is de vereiste mate van zekerheid van de integriteit van belang. Bij het bepalen van de integriteit dient daarom rekening gehouden te worden met de volgende mogelijkheden [4]:

- het voorkomen van schendingen van de integriteit;
- de schade die ontstaat bij schendingen van de integriteit en de mogelijkheden deze schade te beperken;
- de constateerbaarheid van schendingen van de integriteit;
- de reconstructie van een integere situatie wanneer de integriteit is geschonden.

Voor integriteit geldt dat de HIBP onderscheid maakt in:

- de integriteit van de gegevens, zoals die door of namens de eigenaar zijn geaccordeerd (ook wel beeldintegriteit genoemd);
- het handhaven van de integriteit binnen het gegevensverwerkende systeem.

De integriteit van de uiteindelijke resultaten van een gegevensverwerkend systeem is afhankelijk van de volgende factoren [4]:

- de integriteit van de in te voeren gegevens: de integriteit van de in te voeren gegevens is afhankelijk van de initiële integriteit van de aangeleverde gegevens en de integriteit van het proces waarmee de gegevens worden ingevoerd in het gegevens verwerkende systeem;
- de integriteit van de binnen het systeem aanwezige programmatuur en gegevens: de eenmaal in het systeem ingevoerde gegevens dienen integer te zijn en te blijven;
- de integriteit van de geautomatiseerde gegevensverwerking zelf: de integriteit van de in het systeem aanwezige gegevens is afhankelijk van de integriteit van de programmatuur en de systeemdelen van het gegevensverwerkende systeem dient ;
- de integriteit van de nabewerking.

Integriteit wordt binnen de HIBP opgesplitst in [4]:

- volledigheid: volledigheid is de zekerheid dat alle invoer en mutaties worden verwerkt zonder dat er in de gegevensverzamelingen doublures of manco's ontstaan;
- juistheid: juistheid is de zekerheid, dat aangeboden invoer en mutaties correct volgens de specificatie worden verwerkt tot consistente gegevensverzamelingen, zelfs als bewust wordt getracht het informatiesysteem anders te laten functioneren. Juistheid kan worden opgesplitst in werkwijze en functiescheiding;
- actualiteit: actualiteit of tijdigheid is de maximale tijdsduur, die mag liggen tussen het ontstaan en het gebruik van de gegevens, voordat deze gegevens hun waarde verliezen;
- geoorloofdheid: geoorloofdheid van de gegevensverwerking is de zekerheid, dat raadpleging of mutatie van de gegevens of de programmatuur uitsluitend mogelijk is voor personen die daartoe bevoegd zijn.

8.2.1 Procesbeschrijving 'bepalen vereiste/feitelijke integriteit'

In tegenstelling tot het beschikbaarheidsproces zijn bij het integriteitsproces de beschrijvingen van 'bepalen vereiste integriteit' en 'bepalen feitelijke integriteit' samengevoegd. Waarom dit gedaan is, is niet duidelijk in de HIBP aangegeven. Verondersteld wordt dat zowel de vereiste integriteit als de feitelijke integriteit op dezelfde wijze bepaald kan worden.

Binnen de procesbeschrijving wordt uitgegaan van een gegevensverwerkend proces. Dit gegevensverwerkende proces is opgedeeld in een aantal stappen. Per stap is een aantal eisen en/of maatregelen aangegeven met betrekking tot de integriteit van de gegevens binnen dit gegevensverwerkende proces.

Per stap van het gegevensverwerkende proces kan nu bepaald worden welke eisen gelden (en welke maatregelen genomen dienen te worden) voor het bepalen van de vereiste integriteit. Daarnaast kan per stap bepaald worden welke maatregelen getroffen zijn, waardoor de feitelijke integriteit van het proces bepaald kan worden.

8.2.2 Conclusies

De titel 'procesbeschrijving bepalen vereiste/feitelijke integriteit' doet voorkomen dat zowel de vereiste als de feitelijke integriteit met dit proces kan worden bepaald. Het beschreven proces is echter voornamelijk gebaseerd op het bepalen van de vereiste integriteit. De feitelijke integriteit is moeilijker te bepalen met dit proces. Hierbij dient eerst geïnventariseerd te worden welke eisen en maatregelen **zijn** gesteld of getroffen. In de beschrijving wordt vrijwel alleen gesproken over 'eisen/maatregelen die kunnen worden gesteld/getroffen. Voor de inventarisatie van de gestelde eisen en getroffen maatregelen kan wel gebruikgemaakt worden van de opsommingen die binnen de procesbeschrijving zijn opgenomen.

De in de HIBP opgenomen procesbeschrijving is slechts te gebruiken bij database-achtige gegevensverwerkende processen. Binnen de KL is een groot deel van de werkzaamheden niet onder te brengen in dergelijke gegevensverwerkende processen. Gegevens die, tijdens deze werkzaamheden, ingevoerd worden kunnen over het algemeen niet worden gecontroleerd op hun integriteit. De integriteit van deze gegevens is dan ook een verantwoordelijkheid van de persoon die de gegevens invoert.

Gegevens die eenmaal zijn opgenomen in een systeem kunnen wel worden gecontroleerd op ongewenste wijzigingen en geoorloofdheid. Er kan over het algemeen niet worden gecontroleerd op actualiteit, volledigheid en/of juistheid. Hier is de persoon die verantwoordelijk is voor de invoer van de betreffende gegevens tevens verantwoordelijk voor de juistheid, volledigheid en/of actualiteit van deze gegevens.

Het begrip geoorloofdheid heeft een sterke band met het informatiebeveiligingsaspect vertrouwelijkheid. Er dient onderzocht te worden of dit begrip bij exclusiviteit of bij integriteit thuishoort.

8.2.3 Aanbevelingen

Aanbevolen wordt de processen 'bepalen vereiste integriteit' en 'bepalen feitelijke integriteit' afzonderlijk te beschrijven. Hierdoor kan een beter inzicht worden verkregen in de verschillen van beide processen.

Er dient een opsomming te worden opgenomen met informatiebeveiligings bewustwordingsmaatregelen voor functionarissen die werken met gegevensverwerkende processen die niet passen binnen de beschrijvingen die in de HIBP zijn gegeven. Omdat het bij dergelijke processen niet mogelijk of zinloos is om de beschreven integriteitsprocessen uit te voeren is het noodzakelijk dat de informatiebeveiligings bewustwording van functionarissen die met dergelijke processen werken wordt versterkt.

8.3 Evaluatie van het proces 'bepalen feitelijke/vereiste vertrouwelijkheid'

De definitie die de HIBP geeft voor vertrouwelijkheid luidt: de mate waarin de bevoegdheid en de mogelijkheid tot (uit)lezen, kopiëren, verspreiden of kennis nemen van informatie (of andere systeemcomponenten) is beperkt tot een gedefinieerde groep gerechtigden.

Deze groepen worden binnen de HIBP als volgt onderverdeeld [4]:

- rubriceringen: een maat voor schade die ontstaat indien de gegevens in verkeerde handen komen;

- merkingen: aanduiding van de soort machtigingen die nodig zijn om toegang tot de gegevens te kunnen verkrijgen;
- speciale beperkingen: aanduiding van de beperkingen die voor de verspreiding van de gegevens gelden.

Er zijn combinaties van rubriceringen en merkingen mogelijk. In de HIBP is een lijst van mogelijke combinaties opgenomen.

8.3.1 Procesbeschrijving 'bepalen vereiste/feitelijke vertrouwelijkheid'

De HIBP geeft aan dat de eisen die aan een systeem dienen te worden gesteld m.b.t. vertrouwelijkheid op te delen zijn in een aantal gebieden. Eén van deze gebieden betreft het koppelen van computersystemen. Het proces dat in de HIBP beschreven is heeft hier betrekking op en is afgeleid van het proces dat is beschreven in [7]. Hierbij wordt gebruikgemaakt van de beveiligingsklassen, zoals deze gedefinieerd zijn in de 'Trusted Computer System Evaluation Criteria (TCSEC)' [8] ook wel 'Orange book' genoemd.

Binnen het beschreven proces worden 4 stappen onderkend:
- stap 1: het bepalen van de 'mate van blootstelling';
- stap 2: het bepalen van het 'koppelingsrisico';
- stap 3: het bepalen van het 'systeemrisico';
- stap 4: het bepalen van de beveiligingseisen.

Binnen stap 1 wordt gebruik gemaakt van de begrippen vertrouwelijkheidsniveau en machtigingsniveau. Het vertrouwelijkheidsniveau geeft de rubricering en/of merking aan van de gegevens die in een systeem zijn opgeslagen. Het machtigingsniveau geeft het screeningsniveau van de gebruikers aan. Beide begrippen worden in de HIBP geclassificeerd en uitgedrukt in getallen. De 'mate van blootstelling' is nu gelijk aan het verschil tussen het 'hoogste vertrouwelijkheidsniveau' en het 'laagste machtigingsniveau'.

Het bepalen van het 'koppelingsniveau' heeft betrekking op de mogelijkheden die met behulp van de gebruikersapparatuur en de communicatiemiddelen kunnen worden ondersteund. Voor de gebruikersapparatuur wordt onderscheid gemaakt tussen:
- alleen ontvangst;
- interactieve, domme terminal;
- programmeerbaar, d.w.z. toegang via een PC of host.

Voor de communicatieweg wordt het volgende onderscheid gemaakt:
- eenrichtingsverkeer store-and-forward;
- tweerichtingsverkeer store-and-forward;
- interactieve koppeling zonder store-and-forward.

De mogelijke combinaties van mogelijkheden van gebruikersapparatuur en de mogelijkheden van communicatieweg worden weergegeven in een tabel. De combinaties vormen het 'koppelingsrisico' en zijn gewaardeerd door middel van getallen.

Door het 'koppelingsrisico' te combineren met de mogelijkheden van de gebruiker is het mogelijk het 'systeemrisico' te bepalen. De mogelijkheden van de gebruiker zijn:

- alleen uitvoer;
- beperkt interactief;
- programmeermogelijkheden ter beschikking.

Ook hier is een tabel weergegeven van de combinaties van het 'koppelrisico' met de mogelijkheden van de gebruiker en de classificaties van deze combinaties.

Tot slot wordt in stap 4 bepaald welke beveiligingseisen aan het systeem worden toegekend. Dit gebeurt door de 'mate van blootstelling' te koppelen aan het 'systeemrisico'. Hieruit volgt dan de beveiligingsklasse conform de TCSEC die noodzakelijk is voor de afdoende beveiliging van het systeem.

8.3.2 Conclusies

De titel 'procesbeschrijving bepalen vereiste/feitelijke vertrouwelijkheid' doet voorkomen dat zowel de vereiste als de feitelijke vertrouwelijkheid met dit proces kan worden bepaald. Het beschreven proces is echter voornamelijk gericht op het bepalen van de vereiste vertrouwelijkheid. De feitelijke vertrouwelijkheid is moeilijker te bepalen met dit proces. Ook hier zullen de (in het verleden) gestelde eisen en de getroffen maatregelen moeten worden geïnventariseerd. Daarna kan het resultaat van de inventarisatie worden vergeleken met de klassen zoals ze in de procesbeschrijving zijn aangegeven.

De gebruikte methode is gebaseerd op een binnen NATO beproefde methode betreffende de beveiliging van koppelingen van computernetwerken. De klassen (D, C, B en A) die in deze methode worden beschreven zijn afkomstig uit de Trusted Computer System Evaluation Criteria (TCSEC) en vormen een soort basis beveiligingsniveaus (zogenaamde baselines). Deze basis beveiligingsniveaus zijn in het verleden opgesteld vanuit bepaalde (politieke/strategische) overwegingen. Eén van deze overwegingen is gebaseerd op gesloten operationele omgevingen. Gezien gewijzigde omstandigheden, zoals koppelingen met andere netwerken en/of systemen, zijn de destijds opgestelde basis beveiligingsniveaus voor de meeste toepassingen niet meer bruikbaar.

8.3.3 Aanbevelingen

Aanbevolen wordt de processen 'bepalen vereiste vertrouwelijkheid' en 'bepalen feitelijke vertrouwelijkheid' afzonderlijk te beschrijven. Hierdoor kan een beter inzicht worden verkregen in de verschillen van beide processen.

Onderzoeken of de TCSEC basis beveiligingsniveaus nog steeds bruikbaar zijn, waarbij in het bijzonder onderzocht dient te worden of deze beveiligingsniveaus binnen het VIR passen.

9. Conclusies en aanbevelingen

Dit hoofdstuk bevat de conclusies en aanbevelingen die op basis het onderzoek zijn ontstaan.

9.1 Conclusies

Het Voorschrift Informatiebeveiliging Rijksdienst (VIR) is geschreven op een hoog abstractieniveau. De 'Handleiding voor het uitvoeren van heet InformatieBeveiligingsProces' (HIBP) en de KL-methodiek 'Integrale Veiligheids Zorg management' (IVZ-management) zijn praktisch ingesteld. De HIBP kan gezien worden als een praktische invulling van het VIR.

Het VIR geeft aan dat op beleidsniveau de informatiebeveiligingsaspecten geclassificeerd dienen te worden, maar geeft zelf geen classificering aan. Binnen de HIBP en de KL-methodiek IVZ-management worden de informatiebeveiligingsaspecten wel geclassificeerd.

Voor alle methodieken geldt dat de verantwoordelijkheid voor het uitvoeren van de activiteiten, beschreven in deze methodieken, ligt bij het (lijn)management. Binnen de KL betekent dit dat de commandant of afdelingshoofd van het betreffende onderdeel of afdeling verantwoordelijk is voor het uitvoeren van deze activiteiten.

Het VIR en de 'Handleiding voor het uitvoeren van het Informatiebeveiligingsproces' (HIBP) beperken zich beiden tot informatiebeveiliging. De KL-methodiek IVZ-management, daarentegen, is een methodiek die de werkzaamheden beschrijft om te komen tot een adequate beveiliging, in de breedste zin van het woord, van een KL object of lokatie.

De activiteiten en werkzaamheden van het VIR en de HIBP resulteren in het opstellen van een Informatie Beveiligings Plan (IBP). De KL-methodiek IVZ-management heeft tot gevolg dat een bundeling van plannen wordt opgesteld. Eén van die plannen binnen deze bundeling is een IBP.

Uit de omschrijving, die door de KL-methodiek IVZ-management wordt gegeven met betrekking tot het IBP, kan worden opgemaakt dat de invulling van een IBP kan (dient te) worden uitgevoerd conform de HIBP of de MP 10-10 deel 6.

Het VIR en de HIBP gebruiken verschillende benamingen voor dezelfde begrippen.

Met behulp van de subprocessen 1 t/m 5 van de HIBP kan een afhankelijkheidsanalyse, zoals deze beschreven staat in het VIR, worden uitgevoerd. Hierbij dient

opgemerkt te worden dat voor het bepalen van de maximaal toelaatbare schade en de mogelijke schade subproces 4 van de HIBP aangevuld kan worden met de waarde-incident methode en de INCI-DETAR methode van de KL-methodiek IVZ-management en de MP 10-10 deel 3.

Het identificeren en analyseren van bedreigingen kan worden bereikt door subproces 8 van de HIBP uit te voeren. De naam van dit subproces 'Uitvoeren kwetsbaarheidsanalyse' geeft verwarring met de kwetsbaarheidsanalyse volgens het VIR, waarin andere werkzaamheden worden beschreven.

Met de subprocessen 6, 7, 9 en 10 van de HIBP is het mogelijk een kwetsbaarheidsanalyse volgens het VIR uit te voeren.

Voor het opstellen van een Informatie Beveiligings Plan (IBP) kan worden volstaan met het uitvoeren van de subprocessen 11 en 12 van de HIBP. Opgemerkt dient te worden dat de HIBP alle resultaten van alle voorgaande subprocessen in het IBP verwerkt wil zien en het VIR wil slechts een opsomming of verwijzing naar alle te nemen of genomen maatregelen, een calamiteitenparagraaf, audit en control maatregelen en een actieplan.

Door een herindeling van de subprocessen uit te voeren zal de HIBP beter passen binnen de richtlijnen van het VIR. Bij het herindelen van de subprocessen van de HIBP zal tevens onderzocht moeten worden of een uitvoeringsvolgorde van de heringedeelde subprocessen van toepassing is.

De processen voor het bepalen van de feitelijke/vereiste beschikbaarheid, integriteit en vertrouwelijkheid zijn in de praktijk te verwarrend gebleken en dienen vereenvoudigd te worden.

9.2 Aanbevelingen

De volgende aanbevelingen zijn uit het onderzoek naar voren gekomen:

- om in de toekomst verwarringen te voorkomen wordt aanbevolen de begrippen in de HIBP te benoemen conform het VIR;
- pas de indeling van de huidige subprocessen van de HIBP als volgt aan:
  - wijzig de naam van subproces 8 van de HIBP (Uitvoeren kwetsbaarheidsanalyse) in bijvoorbeeld 'Uitvoeren dreigingenanalyse';
  - voeg de subprocessen 6, 7, 9 en 10 samen tot een subproces en noem dit nieuwe subproces 'uitvoeren kwetsbaarheidsanalyse;
  - pas subproces 11 aan door alleen de opsomming van maatregelen of een verwijzing naar de documenten waar deze maatregelen staan vermeld op te nemen in het IBP;
- voor vereenvoudiging van de processen voor het bepalen van de feitelijke/vereiste beschikbaarheid, integriteit en vertrouwelijkheid wordt aanbevolen

deze processen te modificeren door middel van de in het rapport aangegeven wijzigingen.

10. Afkortingenlijst

BA	Beveiligings Autoriteit
BP-IVZ	BasisPlan Integrale VeiligheidsZorg
BVP	Basis Veiligheidszorg Plan
BWP	BeWakings Plan
CO	Centrale Organisatie
DOKL/CIV	Directie Operatiën Koninklijke Landmacht/Commandovoering en Informatie Voorziening
HIBP	Handleiding voor het uitvoeren van het InformatieBeveiligings Proces
HIR	Handboek Informatiebeveiliging Rijksdienst
IBP	Informatie Beveiligings Plan
IVZ	Integrale VeiligheidsZorg
KL	Koninklijke Landmacht
LAS/BO/CIV	LAndmachtStaf/Beleids Ontwikkeling/Commandovoering en Informatie Voorziening (voorheen DOKL/CIV)
MTBF	Mean Time Between Failure
MTTR	Mean Time To Restore
NATCO	NATionaal COmmando
NATO	North Atlantic Treaty Organisation
PLAN-EVO	PLAN Externe Veiligheidszorg Organisatie
PLAN-IVO	PLAN Interne Veiligheidszorg Organisatie
PO BKL 98	ProjectOrganisatie Bewakingssysteem KL 98
PRT	Plan Ressort gebonden Taken
RIPRO	Risico PROfiel
TCSEC	Trusted Computer System Evaluation Criteria
TNO-FEL	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek - Fysisch en Elektronisch Laboratorium
VHZ-BP	VeiligHeidsZorg BasisPlan
VIP	Veiligheidszorg Informatie Pakket
VIR	Voorschrift Informatiebeveiliging Rijksdienst

11. Begrippenlijst

actualiteit	(HIBP) de maximale tijdsduur, die mag liggen tussen het ontstaan en het gebruik van de gegevens (de 'ouderdom'), voordat deze gegevens hun waarde verliezen
afhankelijkheidsanalyse	(VIR) het vaststellen in hoeverre bestuurs- of bedrijfsprocessen die door informatiesystemen ondersteund worden, afhankelijk zijn van de betrouwbaarheid van deze systemen en het vaststellen welke potentiële schades kunnen optreden als gevolg van het falen van deze informatiesystemen
audit en control	(HIBP) de organisatorische, procedurele en instrumentele voorzieningen die benodigd zijn voor de beheersing (verantwoordelijkheden, bevoegdheden, controle en bijsturing) van de beveiliging van de middenlaag
autoriseren	(HIBP) het toekennen van bevoegdheden aan functionarissen voor het gebruik van programmatuur en gegevens. Het autoriseren van functionarissen moet zekerheid geven dat het raadplegen en wijzigen van gevoelige gegevens en de verwerking van deze gegevens uitsluitend mogelijk is door personen, die hiertoe bevoegd zijn. Autorisatie is een belangrijk middel bij het waarborgen van de geoorloofdheid van de informatieverwerking
bedrijfsprocessen	(HIBP) de primaire processen waarvoor de organisatie-eenheid die wordt beschouwd verantwoordelijk is. De ondersteunende processen waar de organisatie-eenheid verantwoordelijk voor is of gebruik van maakt, worden via de relatie meet de primaire processen meegenomen
beschikbaarheid	(VIR) de mate waarin een informatiesysteem in bedrijf is op het moment dat de organisatie het nodig heeft (HIBP) is de mate van ongestoorde voortgang van de informatievoorziening

betrouwbaarheid	(VIR) de mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening
beveiliging	(HIBP) het treffen van maatregelen met als doel het bewerkstelligen en handhaven van veiligheid
beveiligingsmaatregel	(HIBP) maatregel om feitelijke beveiligingsniveau op het gewenste niveau te brengen en te houden
beveiligingsniveau	(HIBP) de mate van beschikbaarheid, vertrouwelijkheid en integriteit, die vanuit het bedrijfsproces is vereist of die vanuit de geautomatiseerde informatievoorziening door de automatiseringsmiddelen kan worden geboden. Het vaststellen van beveiligingsniveaus vindt plaats op basis van de mogelijke schade (sociaal, technisch, organisatorisch, economisch, politiek of infrastructureel) die objecten, processen, personen e.d. ondervinden indien dreigingen zich voordoen
calamiteitenparagraaf	(VIR) opsomming van alle maatregelen welke tot uitvoering moeten komen indien zich een situatie voordoet waarbij de beschikbaarheid, integriteit en/of exclusiviteit van een informatiesysteem in beduidende mate niet aan de eisen voldoen
commandant	(HIBP) voor een operationele eenheid verantwoordelijke functionaris. Hieronder mede te verstaan directeuren en hoofden van niet operationele eenheden
exclusiviteit	(VIR) de mate waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden
geoorloofdheid	de geoorloofdheid van de gegevens verwerking is de zekerheid, dat raadpleging of mutatie van de gegevens of de programmatuur (hetzij rechtstreeks, hetzij via het informatiesysteem) uitsluitend mogelijk is voor personen die daartoe bevoegd zijn. De geoorloofdheid maakt deel uit van het beveiligingsaspect integriteit
incident	(HIBP) het optreden van een ongewenste gebeurtenis of situatie

informatiebeveiliging	(VIR) het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en exclusiviteit van een informatiesysteem en daarmee van de informatie daarin (HIBP) het geheel aan maatregelen met als doel de beheersing van de risico's tijdens verwerking, opslag en overdracht van informatie al dan niet met behulp van geautomatiseerde systemen, teneinde de geëiste vertrouwelijkheid, integriteit en beschikbaarheid te kunnen waarborgen
informatiebeveiligingsplan	(VIR) opsomming van alle beveiligingsmaatregelen en/of de vindplaatsen daarvan welke voor een informatiesysteem of een verantwoordelijkheidsgebied van kracht zijn (HIBP) het rapport waarin de informatiebeveiliging is vastgelegd
informatiesysteem	(VIR) een geheel van gegevensverzamelingen, personen, procedures, programmatuur en opslag-, verwerkings- en communicatieapparatuur (HIBP)
integriteit	(VIR) de mate waarin een informatiesysteem zonder fouten is (HIBP) (betrouwbaarheid, integrity) is de mate waarin de geproduceerde informatie een correcte weergave is van de afgebeelde realiteit en niets ten onrechte is toegevoegd, achtergehouden of verdwenen. Het aspect integriteit is verbijzonderd naar de deelaspecten volledigheid, juistheid, actualiteit (tijdigheid) en geoorloofdheid
juistheid	(HIBP) de zekerheid, dat de aangeboden invoer en mutaties correct volgens specificaties worden verwerkt tot consistente gegevensverzamelingen, zelfs als bewust wordt getracht het informatiesysteem anders te laten functioneren. In geautomatiseerde informatiesystemen kan een grotere mate van juistheid worden bereikt door het uitvoeren van consistentie- en waarschijnlijkheidscontroles
kwetsbaarheidsanalyse	(VIR) het vaststellen van de invloed van het manifest worden van bedreigingen op het functioneren van een

	informatiesysteem of een verantwoordelijkheidsgebied
lijnmanagement	(HIBP) het lijnmanagement is belast met de beheersing van de risico's. Zowel voor de inventarisatie van die risico's als voor wat betreft de implementatie van mogelijke maatregelen kan worden teruggevallen op het instrumentarium. Daarbij stelt het lijnmanagement prioriteiten met betrekking tot de te beveiligen personen, informatie en materieel. Tevens stelt het lijnmanagement vast tot welk beveiligingsniveau maatregelen worden genomen. Ze gaat daarbij uit van een eigen oordeelnorm, maar is gehouden aan de minimaal te nemen maatregelen zoals deze door de beveiligingsautoriteit zijn vastgesteld
middenlaag	(HIBP) het geheel van hardware, software, datacommunicatie, infrastructuren, gegevens, mensen en procedures benodigd om als laag tussen mainframes (bovenlaag) en stand-alone PC's (onderlaag) gegevens te verwerken, op te slaan en te transporteren
risico	(HIBP) de kans op een incident vermenigvuldigd met de daaruit voortvloeiende schade
volledigheid	(HIBP) de zekerheid dat alle invoer en mutaties worden verwerkt zonder dat er in de gegevensverzamelingen doublures of manco's ontstaan
vertrouwelijkheid	(HIBP) (exclusiviteit, confidentiality) is de mate waarin de bevoegdheid en de mogelijkheid tot (uit)lezen, kopiëren, verspreiden of kennis nemen van informatie (of andere systeemcomponenten) is beperkt tot gedefinieerde groep gerechtigden

12. Referenties

[1] Voorschrift Informatiebeveiliging Rijksdienst 1994

[2] Handboek Informatiebeveiliging Rijksdienst

[3] Beleidsdocument Informatiebeveiliging versie 1.0, Ministerie van Defensie, 30 november 1995

[4] Handleiding voor het uitvoeren van het InformatieBeveiligingsProces, Directie Operatiën Koninklijke Landmacht afdeling Commandovoering en Informatie Voorziening (DOKL/CIV), 4 november 1993

[5] Concept memorandum KL methodiek Integrale VeiligheidsZorg Management (versie 2.2), Nationaal Commando ProjectOrganisatie Bewakingssysteem KL 98 (NATCO/PO BKL 98), 20 maart 1996

[6] Ministeriële Publicatie MP 10-10 concept deel 6: Beveiliging van geautomatiseerde gegevensverwerkende systemen, Ministerie van Defensie, 30 januari 1992

[7] AC/35-D1022, NATO provisional security policy guidance on the interconnection of networks, 1993

[8] Trusted Computer System Evaluation Criteria (TCSEC), Department of Defense USA, december 1985

13. Ondertekening

D.W. Fikkert
Groepsleider

P.J.A. Verhaar
Auteur

REPORT DOCUMENTATION PAGE
(MOD-NL)

1. DEFENCE REPORT NO (MOD-NL)	2. RECIPIENT'S ACCESSION NO	3. PERFORMING ORGANIZATION REPORT NO
TD97-0092		FEL-97-A066
4. PROJECT/TASK/WORK UNIT NO	**5. CONTRACT NO**	**6. REPORT DATE**
6024030	A94KL646	April 1997
7. NUMBER OF PAGES	**8. NUMBER OF REFERENCES**	**9. TYPE OF REPORT AND DATES COVERED**
52 (excl RDP & distribution list)	8	

10. TITLE AND SUBTITLE

Evaluatie KL informatiebeveiligingsmethodieken in relatie tot het Voorschrift Informatiebeveiliging Rijksdienst (VIR)
(Evaluation RNLA information security methodologies related to the VIR (information security regulations for government use))

11. AUTHOR(S)

P.J.A. Verhaar

12. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

TNO Physics and Electronics Laboratory, PO Box 96864, 2509 JG The Hague, The Netherlands
Oude Waalsdorperweg 63, The Hague, The Netherlands

13. SPONSORING AGENCY NAME(S) AND ADDRESS(ES)

Royal Netherlands Army
LAS/BO/CIV, PO Box 90711, 2509 LS The Hague, The Netherlands

14. SUPPLEMENTARY NOTES

The classification designation Ongerubriceerd is equivalent to Unclassified, Stg. Confidentieel is equivalent to Confidential and Stg. Geheim is equivalent to Secret.

15. ABSTRACT (MAXIMUM 200 WORDS (1044 BYTE))

The security authority of the Dutch Ministry of Defense drew up the information security policy document 'Beleidsdocument Informatiebeveiliging'. This document was drew up according to the 'Voorschrift Informatiebeveiliging Rijksdienst' (VIR - information security regulations for government use), and is operative for the entire Dutch military force.
The Army Staff has requested TNO-FEL to compare two security methodologies to the policy framework described in the policy document. It concerns the methodologies: 'Handleiding voor het uitvoeren van het informatiebeveiligingsproces' from the Army Staff (LAS/BO/CIV), and 'KL-methodiek Integrale Veiligheidszorg management' from the National Command (NATCO) of the Netherlands Army.
TNO-FEL has studied whether the methodologies comply with the activities described in the VIR. TNO-FEL also studied the methodologies for resemblances and differences.

16. DESCRIPTORS	IDENTIFIERS
Security Information systems Regulations	Information security Risk analysis

17a.SECURITY CLASSIFICATION (OF REPORT)	17b.SECURITY CLASSIFICATION (OF PAGE)	17c.SECURITY CLASSIFICATION (OF ABSTRACT)
Ongerubriceerd	Ongerubriceerd	Ongerubriceerd

18. DISTRIBUTION AVAILABILITY STATEMENT

Unlimited Distribution

17d.SECURITY CLASSIFICATION (OF TITLES)

Ongerubriceerd

Distributielijst

1.	Bureau TNO Defensieonderzoek
2.	Directeur Wetenschappelijk Onderzoek en Ontwikkeling*)
3.	HWO-KL
4.	HWO-KLu*)
5.	HWO-KM*)
6.	HWO-CO*)
7 t/m 9.	KMA, Bibliotheek
10.	LAS/BO/CIV, t.a.v. Ing. J.P.H.M. Klomp
11.	LAS/BO/CIV, t.a.v. Kol Oude Lohuis
12 t/m 31.	CO/BA t.a.v. voorzitter en leden BEVCIS
32.	HMID, t.a.v. Mr. J.C.F. Knapp
33.	DCAKL, t.a.v. Kol Langenhuizen
34.	DCAKL/ITO, t.a.v. Ir. G. Kanning
35.	NATCO/Integrale Beveiligingscoördinator KL
36.	NATCO/OI&T, t.a.v. Lkol A.A.M. Struijk
37.	NBV, t.a.v. Dhr. N. Plasier
38.	DCC, t.a.v. Ir. H.I.M. Nieuwenhuis MBA
39.	DEFAC, EDP-audit, t.a.v. Dhr. R. Daalder
40.	OC EDE C^3 EOV, t.a.v. LKol Adolf
41.	Archief TNO-FEL, in bruikleen aan M&P*)
42.	Directie TNO-FEL, t.a.v. Dr. J.W. Maas
43.	Directie TNO-FEL, t.a.v. Ir. J.A. Vogel, daarna reserve
44.	Archief TNO-FEL, in bruikleen aan D.W. Fikkert
45.	Archief TNO-FEL, in bruikleen aan Ir. H.A.M. Luiijf
46.	Archief TNO-FEL, in bruikleen aan Ir. E. Hardam
47.	Archief TNO-FEL, in bruikleen aan Ing. P. Verhaar
48.	Archief TNO-FEL, in bruikleen aan Ir. F. Nielen
49.	Archief TNO-FEL, in bruikleen aan Ir. P. Franken
50.	Documentatie TNO-FEL
51 t/m 54.	Reserve
	TNO-PML, Bibliotheek**)
	TNO-TM, Bibliotheek**)
	TNO-FEL, Bibliotheek**)

Indien binnen de krijgsmacht extra exemplaren van dit rapport worden gewenst door personen of instanties die niet op de verzendlijst voorkomen, dan dienen deze aangevraagd te worden bij het betreffende Hoofd Wetenschappelijk Onderzoek of, indien het een K-opdracht betreft, bij de Directeur Wetenschappelijk Onderzoek en Ontwikkeling.

*) Beperkt rapport (titelblad, managementuittreksel, RDP en distributielijst).
**) RDP.